

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

昭64-28672

⑬ Int. Cl.⁴ 識別記号 庁内整理番号 ⑭ 公開 昭和64年(1989)1月31日
G 09 C 1/00 7368-5B
G 06 F 15/21 310 Z-7230-5B
H 04 L 9/00 Z-7240-5K 審査請求 未請求 発明の数 2 (全4頁)

⑮ 発明の名称 電子取引用認証方式

⑯ 特 願 昭62-183278

⑰ 出 願 昭62(1987)7月24日

⑱ 発 明 者 永 井 康 彦 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

⑲ 発 明 者 宝 木 和 夫 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

⑳ 発 明 者 佐々木 良一 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

㉑ 出 願 人 株式会社日立製作所 東京都千代田区神田駿河台4丁目6番地

㉒ 代 理 人 弁理士 小川 勝男 外1名

明 細 書

1. 発明の名称

電子取引用認証方式

2. 特許請求の範囲

1. 詳細な電気的情報に置き換えて、電子的に所望の取引を行ない、かつ取引文の内容を示すデータを公伝送時方式を用いて暗号化することで認証データを作成、復号することで認証データの検証をする電子取引用認証方式において、復号用公伝送には、暗号化用秘密鍵よりも短い鍵長のものを採用し、認証データ作成には、剰余テーブルを用いた高速剰余計算方式、認証データ検証には従来方式の剰余を求めて被除数から除性する方式を採用することにより、認証データ作成・検証処理の高速化を可能とすることを特徴とする電子取引用認証方式。

2. ホスト対端末が1:n (n:正整数)であるような通信ネットワークを持つ電子取引方式において、ホスト側や取引頻度の高い端末側では認証データ作成用に上記剰余テーブルを用いた

剰余計算方式を採用することを特徴とする電子取引用認証方式。

3. 発明の詳細な説明

(産業上の利用分野)

本発明は、データをコンピュータのメッセージに置き換え、電子的に荷取引を行ない、公開鍵暗号方式による取引データの認証を行なう電子取引用認証方式において、特にホスト1に対し相手端末がnであるような通信ネットワーク上の認証処理の高速化、高効率化に適する。

(従来の技術)

従来、荷取引による契約交渉は、サイン・印鑑によりその正当性を認証している。この作業をデジタル通信を利用した電子取引で実現する方法が考案されているが、サイン・印鑑のデータをそのままデジタル信号に変換して使用することは、取引の信頼性の面から問題を生じる。これは、サイン・印鑑のデジタル信号化されたデータは、簡単にその複製を作成することができるため、その複製物により不正な取引を行なうことが容易なため

である。そこで、サイン・印鑑のデータの単純なデジタル信号化に変わる手段としてデジタル署名を用いる手段が有力とされている。デジタル署名とは、認証を行ないたい情報（取引当事者の氏名や取引内容）に暗号化処理を行なって作成した暗号文で、この暗号化の際に用いた暗号化鍵を知らない第三者には、作成することが困難なものであるという事実から、その作成者を認証・特定化するものである。

現在、このデジタル署名を実現するために最も有力な暗号方式は、公開鍵暗号方式である。公開鍵暗号方式では、データ（平文）を暗号化する鍵と暗号化されたデータ（暗号文）を復号する鍵の両者が異なっているという特徴がある。そのため、暗号化鍵は秘密し、復号鍵を公開しておくことにより、秘密の第三者に暗号化鍵を秘密したままでも認証をさせることができる（（財）日本情報処理開発協会：「コンピュータ・システムのセキュリティ技術の開発に関する調査研究報告書」昭和59、3参照）。

端末において認証データ作成に剰余テーブルを用いた多倍長剰余計算高速化方式を採用する。

〔作用〕

公開鍵に秘密鍵よりも短い鍵長のものを採用することにより、認証データ確認処理の計算量を減少させ、高速化が達成できる。また、取引データの処理量が多いホストや端末において認証データ作成処理に剰余テーブルを用いた剰余計算高速化方式を採用することで、通信ネットワーク全体としての取引の高速化、高効率化が達成できる。

〔発明の実施例〕

以下、本発明の一実施例について、その概略、動作を第1図及び第2図を用いて説明する。

第1図は、投資家（端末）と証券会社（ホスト）を通信ネットワークで結ぶ株式売買システムに本発明を適用した場合の構成を示している。

公開鍵暗号処理用暗号機としては、比較的低速ではあるが小型で実現できる方式、高速ではあるがメモリ容量を多く必要とする方式という2つの方式のものがある。投資家側端末では、取引頻度

〔発明が解決しようとする問題点〕

従来、上記公知例に代表されるような公開鍵暗号方式を用いたデジタル署名には、一般に公開鍵暗号方式が多倍長の剰余計算を計算単位とし、計算量が多いため処理速度の面で実用化が困難であるという問題があり、運用面での効率的な実用化方法も検討されていない。

本発明の目的は、多倍長剰余算を計算単位とする公開鍵暗号方式を用いた電子認証方式において、運用面での高速、高効率処理を実現し、実用的な電子取引用認証方式を提供することにある。

〔問題を解決するための手段〕

上記目的を達成するため、本発明による電子取引用認証方式では、公開鍵暗号方式の公開鍵に秘密鍵より鍵長の短いものを採用する。公開鍵は、暗号者に公開される暗号鍵であるため、鍵長を短くしても実用上安全性に問題は無い。これにより、認証データ確認のための計算量を減少させる。また、電子取引を行なう通信ネットワーク内で、取引文データが集中するホストや、取引頻度の高い

が少ないことから、従来の比較的低速の公開鍵暗号処理用暗号機Aを用い、認証データの作成・確認を行なう。一方、証券会社であるホスト側では、認証データの確認用の公開鍵は作成用秘密鍵よりも鍵長が短いことから計算量が少ないため、認証データの確認には高速の暗号機Bを採用し、認証データ作成には、剰余テーブルを用いた高速処理用暗号機Bを用いる。

第2図は、端末側、ホスト側の構成要素及び処理フローを示している。

ステップ1：まず投資家側端末101において、

注文伝票の内容を示すデータ及び取引状況を示すデータ等より認証データ原文を作成し、また、記憶装置103より投資家側秘密鍵を暗号機A104にロードして投資家側認証データを暗号化することにより作成する。

ステップ2：次に作成された認証データを記憶装

親103に登録すると共に通信制御装置105より証券会社側へ送信する。

ステップ3：証券会社側は、通信制御装置105より投資家の認証データを受信し、記憶装置107へ登録する。

ステップ4：次に暗号機A108に記憶装置より認証データ及びそのデータの送信元である投資家に対応した公開鍵をロードし、認証データを復号して原文を得る。

ステップ5：得られた認証データ原文を比較器109により確認し、妥当であれば証券会社側の認証データ原文を作成器110より作成する。

ステップ6：ホスト側秘密鍵を記憶装置107より暗号機B111にロードし、会社側認証データを作成する。

ステップ7：通信制御装置105より投資家側へ認証データを送信する。

ステップ8：会社側認証データを通信制御装置

105より受信し、記憶装置103よりホスト公開鍵を暗号機A104にロードして認証データの復号を行う。

ステップ9：復号結果である認証原文を比較器

112より認証し、妥当であれば認証データを記憶装置103に登録する。

以上により作成・確認した双方の認証データを双方が保管しておくことにより、本取引は保証される。なお、本実施例では2種類の暗号機A、Bを使用した。剰余テーブルを用いた高速化方式が、今後小型、低コストで実現可能になれば、全てを暗号機Bにすることにより一層高速化が望める。また、本方式は、電子取引における認証機能だけでなく、一般的に公開鍵暗号方式を応用した各種機能を実現する場合においても有効である。
(発明の効果)

本発明によれば、復号用公開鍵には暗号化用秘密鍵よりも短い鍵長のものを採用したことにより、認証データ確認処理の計算量を減少させ、高速化が実現でき、また、多量の取引文を処理するホスト側や取引頻度の高い端末側において認証データ作成のため剰余テーブルを用いた公開鍵暗号高速処理方式を採用することにより、通信ネットワークータルとしての取引の高速化、高効率化を実現できるという効果がある。

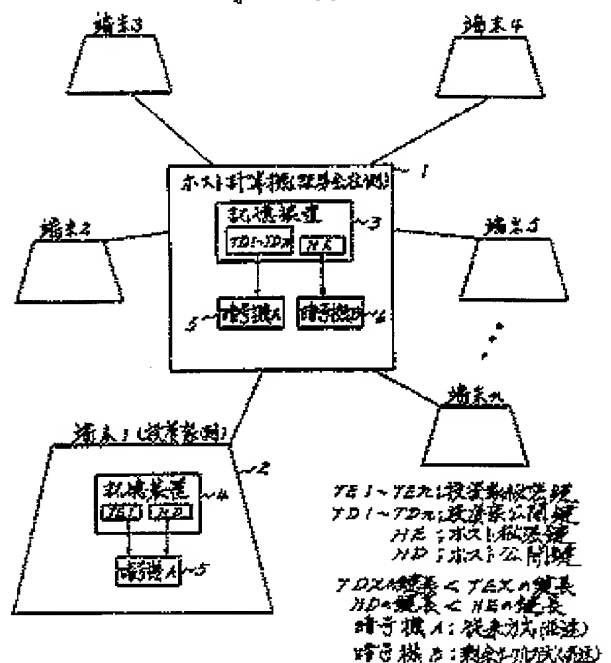
4. 図面の簡単な説明

第1図は、本発明による株式売買システムの一構成図、第2図は、その構成要素及び処理フロー図である。

代理人 井原士 小川藤男



第1図



第2図

